RADemics

Hybrid AI Architectures Combining ML and DL for Insider Threat Detection

S.Sivakumar, B.Persis Urbana Ivy , Srikanta Kumar Sahoo

SRM Institute of Science and Technology, Mother Teresa Institute of Engg and Technology,Melumoi (Post), Bhubaneswar Engineering College

Hybrid AI Architectures Combining ML and DL for Insider Threat Detection

[1]S. Sivakumar, Assistant Professor, School of Computing, SRM Institute of Science and Technology -Tiruchirappalli. shivakumar@gmail.com

[2]B. Persis Urbana Ivy, Dean (CSE & Allied branches), Mother Teresa Institute of Engg and Technology, Melumoi (Post), Palamaner - 517408, sperurban.mti@gmail.com.

[3]Srikanta Kumar Sahoo, Asst. Prof., CSE, Bhubaneswar Engineering College, Bhubaneswar, Odisha. skskumar.nita@gmail.com

Abstract

The rapid evolution of insider threats presents a significant challenge for cybersecurity systems, necessitating the development of advanced detection models capable of adapting to dynamic and sophisticated attack patterns. This chapter explores the integration of Hybrid Artificial Intelligence (AI) architectures combining Machine Learning (ML) and Deep Learning (DL) with emerging techniques such as Reinforcement Learning (RL) to enhance insider threat detection. The combination of ML and DL methodologies offers distinct advantages in handling large, complex datasets, while RL introduces the capability for real-time adaptation to evolving threat behaviors. By leveraging hybrid models, organizations can better detect subtle insider threats that traditional systems often fail to identify, improving accuracy and response times. Despite the promise, challenges such as model interpretability, data privacy, and the exploration-exploitation trade-off in RL systems must be addressed. The chapter discusses these hurdles and provides insights into how hybrid architectures can be optimized to overcome them, with a focus on scalability, security, and the ability to continuously learn from new data. Through a comprehensive review of the current research and methodologies, this chapter aims to highlight the potential of hybrid AI models in revolutionizing the way insider threats are detected and mitigated in real-time, offering a path toward more resilient and adaptive cybersecurity systems.

Keywords: Insider Threat Detection, Hybrid AI, Machine Learning, Deep Learning, Reinforcement Learning, Cybersecurity.

Introduction

The evolving nature of insider threats represents one of the most critical challenges in modern cybersecurity [1]. Unlike traditional external threats, which target systems from outside an organization’s trusted perimeter, insider threats come from within, often with a deeper understanding of the system and its vulnerabilities [2]. These threats may stem from disgruntled employees, careless actions, or even external actors exploiting insiders [3]. The complexity and subtlety of insider threats make them difficult to detect using conventional security measures, which typically focus on perimeter defense. As a result, organizations need more sophisticated, adaptive systems capable of identifying malicious behavior at an early stage [4]. Hybrid artificial intelligence (AI) architectures that combine machine learning (ML), deep learning (DL), and reinforcement learning (RL) have shown great promise in addressing these challenges. By leveraging the strengths of these techniques, hybrid models can detect both known and novel insider threats, providing a dynamic and proactive defense mechanism [5].

Traditional security models, which often rely on rule-based or signature-based approaches, are limited in their ability to detect emerging insider threats [6]. These models struggle with detecting unknown attack patterns, particularly when the threat actors exhibit behaviors that closely resemble legitimate user activity [7]. Machine Learning (ML) and Deep Learning (DL) models offer more flexibility, as they are designed to learn from data and can recognize complex, non-linear relationships that may not be immediately apparent [8]. ML models, such as decision trees and support vector machines, excel at identifying patterns based on historical data, while DL models, particularly deep neural networks, are adept at learning from unstructured data like system logs, user behavior patterns, and network traffic. However, while these methods are powerful, they have limitations in handling dynamic, real-time threats that evolve over time [9]. This is where Reinforcement Learning (RL) can make a significant contribution, as it allows models to continuously adapt by learning from interactions with the environment, responding to new threats as they arise [10].

The integration of Reinforcement Learning into hybrid models allows for a continuous learning process, enabling the system to adapt in real time to new and evolving insider threats [11]. Unlike traditional machine learning methods, which require retraining with large labeled datasets, RL models can update their strategies autonomously by interacting with real-time data [12]. In the context of insider threat detection, this means that the model can adjust its detection strategies based on new behavioral patterns or tactics employed by malicious insiders [13]. For instance, RL-based systems can learn to prioritize certain behaviors, such as unusual access to sensitive data or abnormal system interactions, by assigning rewards to actions that lead to successful threat detection [14]. This dynamic adaptation improves the system’s ability to identify new attack vectors that might otherwise go unnoticed by static, rule-based models. RL allows the model to balance exploration and exploitation, making it capable of discovering novel attack patterns while still capitalizing on known detection strategies [15].